IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

UNITED STATES OF AMERICA	)	
	)	22-1808-ADC
v.	)	Case No.: _____
	)	
The Domain Name **KingsmarkPharma.com**	)	
	)	
	)	

AFFIDAVIT IN SUPPORT OF SEIZURE WARRANT

I, Ryan DiAndrea, being duly sworn, hereby declare as follows:

INTRODUCTION AND AGENT BACKGROUND

1. Your Affiant is a Special Agent with Homeland Security Investigations (HSI) and have been so employed since June 2016. I am a graduate of the Criminal Investigator Training Program (CITP) and the HSI Special Agent Training (SAT) Program at the Federal Law Enforcement Training Center in Glynco, Georgia. I have a Bachelor of Science degree in business administration, and a Master of Business Administration degree. Prior to my current assignment, I was assigned to HSI Laredo where I was tasked with investigating crimes which primarily pertained to human smuggling and drug trafficking. I am currently assigned to the HSI Baltimore Transnational Cyber Crimes Team (TCCT). Pursuant to this assignment, I am primarily tasked with investigating criminal activity that is facilitated through the use of the internet, the dark web and digital currencies which pertain to the international importation, possession, and distribution of prohibited materials, including but not limited to illicit or counterfeit goods (including but not limited to pharmaceuticals), narcotics and narcotics manufacturing paraphernalia.

2. Your affiant is an investigative or law enforcement officer of the United States within the meaning of 18 U.S.C. § 2510(7) and empowered by law to conduct investigations and

to make arrests for offenses enumerated in 18 U.S.C. § 2320 (Trafficking in counterfeit goods or services). In the course of my training and experience, I have become familiar with the methods and techniques associated with the distribution of counterfeit goods narcotics, the laundering of drug proceeds, and the organization of drug conspiracies.

3. As a result of my training and experience, I have learned about the importation, manufacture and distribution of counterfeit goods. I have participated in investigations involving the laundering of monetary instruments and smuggling of bulk United States currency.

4. In the course of conducting those investigations, I have been involved in the use of the following investigative techniques: interviewing informants and cooperating witnesses, conducting physical surveillance, consensual monitoring and recording of both telephonic and non-telephonic communications, analyzing telephone pen register and caller identification system data, conducting court-authorized electronic surveillance (including wire interceptions), and preparing and executing search warrants that have led to seizures of narcotics, currency, firearms, and other contraband.

5. Through my training and experience, I have become familiar with the manner in which counterfeit goods are manufactured, transported, stored, and distributed, and with the method of payment for such goods. I have also become familiar with the means and methods in which counterfeit goods traffickers transport, deposit, and collect the illicit proceeds. I am familiar with the support and assistance that illicit organizations require to conduct their illegal activities. I have also become knowledgeable about the criminal statutes of the United States, particularly in the area of the law relating to violations of the federal counterfeit goods, narcotics and conspiracy statutes.

6. The facts in this Affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This Affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter or investigation. I have not, however, excluded any information known to me that would defeat a determination of probable cause. Moreover, where, in this report your Affiant described or referred to a statement made by an individual, that statement is described in substance and in part—it is not intended to be a verbatim recitation of the entire statement made by that individual.

7. As set forth below, there is probable cause to believe that the domain "https://www.KingsmarkPharma.com," **("SUBJECT DOMAIN NAME**") is property used, or intended to be used, to commit or facilitate violations of 18 U.S.C. § 2320 (Trafficking in counterfeit goods or services), and subject to seizure and forfeiture pursuant to 18 U.S.C. § 2323. I make this Affidavit for a warrant to seize the property described in ATTACHMENT A, specifically, the **SUBJECT DOMAIN NAME**.

8. The procedure by which the Government will seize the **SUBJECT DOMAIN NAME** is described in ATTACHMENT A hereto and below.

BACKGROUND

9. Based on my training and experience and information learned from others, I am aware of the following terms that are relevant to understanding this investigation:

10. Internet Protocol Address: An Internet Protocol address ("IP address") is a unique numeric address used by computers on the Internet. An IP Address is a series of four numbers, each in the range 0-255, separated by periods (*e.g.*, 121.56.97.178). Every computer

connected to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. An IP address acts much like a home or business street address; it enables computers connected to the Internet to properly route traffic to each other. The assignment of IP addresses to computers connected to the Internet is controlled by Internet Service Providers.

11. Domain Name: A domain name is a simple, easy-to-remember way for humans to identify computers on the Internet, using a series of characters (*e.g.*, letters, numbers, or other characters) that correspond with a particular IP address. For example, "usdoj.gov" and "cnn.com" are domain names.

12. Domain Name System: The domain name system ("DNS") is, among other things, a hierarchical convention for domain names. Domain names are composed of one or more parts, or "labels," that are delimited by periods, such as "www.example.com." The hierarchy of domains descends from right to left; each label to the left specifies a subdivision, or subdomain, of the domain on the right. The right-most label conveys the "top-level" domain. For example, the domain name "www.example.com" means that the computer assigned that name is in the ".com" top-level domain.

13. Domain Name Servers: DNS servers are computers connected to the Internet that convert, or resolve, domain names into IP addresses.

14. Registry: For each top-level domain (such as ".com"), there is a single company, called a "registry," that determines which second-level domain resolves to which IP address. For example, the registry for the ".com" and ".net" top-level domains are VeriSign, Inc., which has its headquarters at 12061 Bluemont Way, Reston, Virginia.

15. Registrar & Registrant: Domain names may be purchased through a registrar, which acts as the intermediary between the registry and the purchasers of the domain name. The individual or business that purchases, or registers, a domain name is called a "registrant." Registrants control the IP address, and thus the computer, to which their domain name resolves. Thus, a registrant may easily move a domain name to another computer anywhere in the world. Typically, a registrar will provide a registrant with the ability to change the IP address. . Registrars typically maintain customer and billing information about the registrants who used their domain name registration services.

16. Whois: A "Whois" search provides publicly available information as to which entity is responsible for a particular IP address or domain name. A Whois record for a particular IP address or domain name will list a range of IP addresses that that IP address falls within and the entity responsible for that IP address range and domain name. For example, a Whois record for the domain name XYZ.COM might list an IP address range of 12.345.67.0- 12.345.67.99 and list Company ABC as the responsible entity. In this example, Company ABC would be responsible for the domain name XYZ.COM and IP addresses 12.345.67.0- 12.345.67.99.

17. Phishing: "Phishing" is a common form of social engineering used to induce victims into turning over sensitive data—such as personally identifiable information, passwords, and credit card details. Victims of phishing attacks are generally contacted by email, phone, or text message by persons purporting to be from reputable companies in order to induce the victims to reveal confidential data. Phishing emails commonly are designed to appear as if they originate from a legitimate source, such as a well-known business, and direct the recipient to a fraudulent website link. Like the email itself, the fraudulent website has the façade of legitimacy,

but the fake site is designed to induce victims to personal information, such as usernames and passwords linked to an organization's authentic website. This information is then captured by the scammer.

18. Uniform Resource Locator: A Uniform Resource Locator (URL), colloquially termed a web address, is a reference to a web resource that specifies its location on a computer network and a mechanism for retrieving it. A URL is a specific type of Uniform Resource Identifier (URI), although many people use the two terms interchangeably.

19. Internet Corporation for Assigned Names and Numbers: The Internet Corporation for Assigned Names and Numbers (ICANN) is an American multi-stakeholder group and nonprofit organization responsible for coordinating the maintenance and procedures of several databases related to the namespaces and numerical spaces of the Internet, ensuring the network's stable and secure operation.

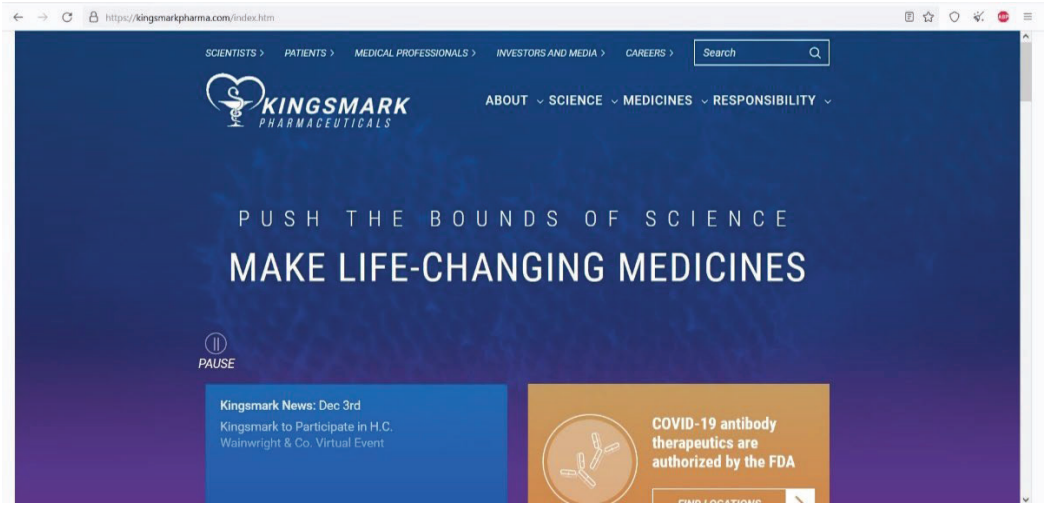
CASE BACKGROUND

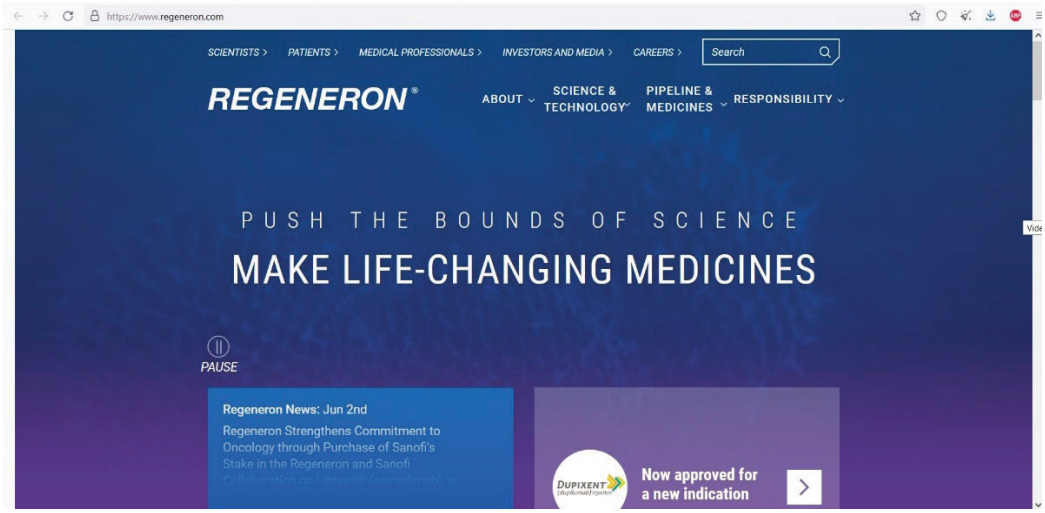
20. In late 2019, a novel coronavirus, SARS-CoV-2, was first detected in Wuhan, China, causing outbreaks of the disease COVID-19 that have since spread globally. COVID-19 is highly contagious and causes severe acute respiratory syndrome. On March 13, 2020, the President of the United States declared a national emergency due to the COVID-19 pandemic.

21. REGN-COV2 is an antibody drug cocktail utilized for the treatment of COVID-19. Regeneron developed the REGEN-COV2 antibody drug cocktail, which consists of casirivimab and imdevimab. Regeneron is headquartered in Tarrytown, New York. Regeneron is a biotech company that develops treatments for a number of different ailments. In November 2020, The U.S. Food and Drug Administration (FDA) granted emergency use authorization of

REGEN-COV2 the for the treatment of COVID-19.

22. The HSI Intellectual Property Rights Center ("IPRC") and the HSI Cyber Crimes Center ("C3") became aware of an apparent fraudulent website, named "KingsmarkPharma.com" (**SUBJECT DOMAIN NAME**). Regeneron confirmed that the **SUBJECT DOMAIN NAME** is not a legitimate Regeneron website. A screenshot of the homepage for the **SUBJECT DOMAIN NAME** (top) compared to the legitimate Regeneron homepage (https://www.regeneron.com) (bottom) is included below:

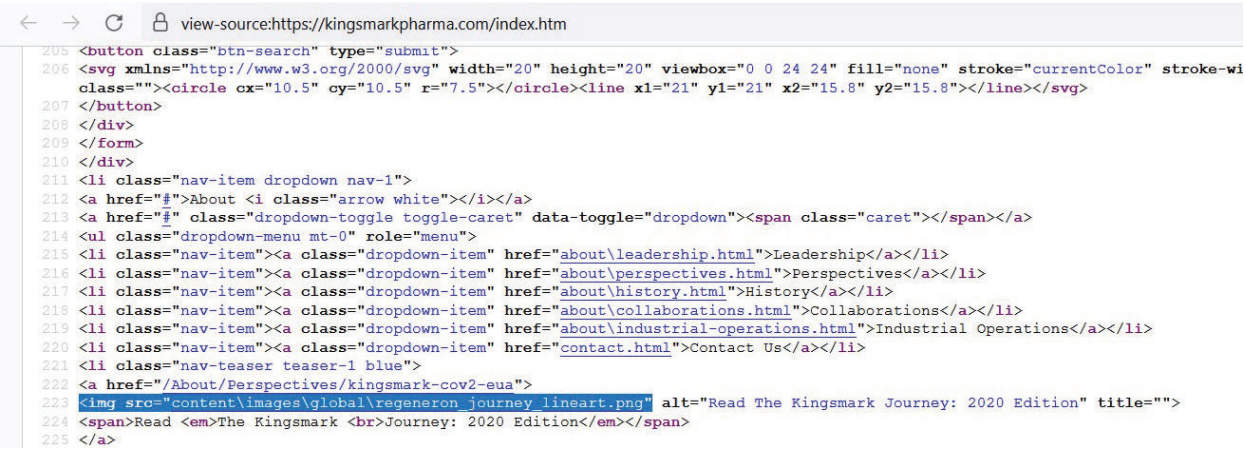




23. On June 3, 2022, your affiant accessed the **SUBJECT DOMAIN NAME** while located in Maryland.

24. A domain analysis conducted by your affiant indicated the **SUBJECT DOMAIN NAME** was created on or about December 2, 2021, and the registrar was listed as NameCheap, Inc., whose headquarters are located in Phoenix, Arizona. The Registrant was listed as being "redacted for privacy."

25. Your affiant conducted a review of the **SUBJECT DOMAIN NAME's** online content, which is designed to mimic the style and design of the legitimate Regeneron website. Portions of the source code for the **SUBJECT DOMAIN NAME** website appear to have been copied and mirrored off the legitimate Regeneron website. It appears that the individual stealing the source code from the Regeneron website replaced most references to "Regeneron" with "Kingsmark" or "Kingsmark Pharmaceuticals." Screenshots of the homepage source code for the **SUBJECT DOMAIN NAME** (top) compared to the source code for the legitimate Regeneron homepage (https://www.regeneron.com) (bottom) are included below:



26. Your affiant noted that a number of links or buttons on the **SUBJECT DOMAIN NAME** website did not function as expected while the same buttons and links function properly on the legitimate Regeneron website.

27. Your affiant navigated to an index directory page on the **SUBJECT DOMAIN NAME** located at: https://kingsmarkpharma.com/content/images/about/leadership/ and observed that the index contained 54 .jpg and .png files that are images of legitimate Regeneron executives such as George Yancopoulos and Leonard S. Schleifer, the founders of Regeneron. The index directory page also contains 17 .jpeg files that appear to be randomly selected individuals to represent the fictious leadership team of Kingsmark Pharmaceuticals.

28. An analysis conducted by a Cyber Operations Officer (COO) utilized specialized threat analysis tools and discovered multiple threats such as phishing, spam and malware were present on the **SUBJECT DOMAIN NAME** website.

29. Based on training, experience and information obtained from other law enforcement agents and officers, your Affiant believes this website was set up for the purpose of collecting customers' personal identification in order to use that information for nefarious purposes such as fraud, which could include phishing attacks and/or deployment of malware.

THE SUBJECT DOMAIN NAME

30. As described above, the **SUBJECT DOMAIN NAME** was used by unknown

subjects to commit violations of 18 U.S.C. § 2320.

31. Your Affiant conducted a search of publicly available Whois domain name registration records. That search revealed that the **SUBJECT DOMAIN NAME** was registered on or about December 2, 2021, through the registrar NameCheap, Inc., which according to their website, is headquartered in Phoenix, Arizona. The publicly available Whois database did not list a registrant or contact information for the **SUBJECT DOMAIN NAME**. VeriSign, Inc., (the **SUBJECT REGISTRY**) is the top-level registry for all ".com" domains, headquartered at 12061 Bluemont Way, Reston, VA 20190. It is known by agents that criminals who operate websites and use targeted domain names, such as the **SUBJECT DOMAIN NAME**, often conceal their identity when registering their domain names by redacting personal identifiers to avoid being tracked by victims or law enforcement.

32. As detailed in ATTACHMENT A, upon execution of the seizure warrant, VeriSign Inc., the registry for the ".com" top-level domain, shall be directed to restrain and lock the **SUBJECT DOMAIN NAME** pending transfer of all right, title, and interest in the **SUBJECT DOMAIN NAME** to the United States upon completion of forfeiture proceedings, to ensure that changes to the **SUBJECT DOMAIN NAME** cannot be made absent court order or, if forfeited to the United States, without prior consultation with HSI or the Department of Justice ("DOJ").

33. In addition, upon seizure of the **SUBJECT DOMAIN NAME** by Homeland Security Investigations, VeriSign Inc., will be directed to associate the **SUBJECT DOMAIN NAME** to a new authoritative name server(s) to be designated by a law enforcement agent. The Government will display a notice on the website to which the **SUBJECT DOMAIN NAME** will

resolve indicating that the site has been seized pursuant to a warrant issued by this Court.

STATUTORY BASIS FOR SEIZURE AND FORFEITURE

34. 18 U.S.C. § 2323(a) provides, in relevant part, that any property used, or intended to be used, in any manner or part to commit or facilitate the commission of an offense in violation of 18 U.S.C. § 2320 is subject to civil forfeiture to the United States government.

35. 18 U.S.C. § 981(b), as incorporated by 18 U.S.C. § 2323(a)(2), authorizes the seizure of property subject to civil forfeiture based upon a warrant supported by probable cause. 18 U.S.C. § 981(b)(3), as incorporated by 18 U.S.C. § 2323(a)(2), permits the issuance of a seizure warrant by a judicial officer in any district in which a forfeiture action against the property may be filed and may be executed in any district in which the property is found.

36. 18 U.S.C. § 2323(b) provides, in relevant part, that any property used, or intended to be used, in any manner or part to commit or facilitate the commission of an offense in violation of 18 U.S.C. § 2320 is subject to criminal forfeiture to the United States government.

37. 18 U.S.C. § 2323(b)(2) authorizes the issuance of a criminal seizure warrant under 21 U.S.C. § 853(f), which provides, in relevant part, that a seizure warrant for property subject to forfeiture may be sought in the same manner in which a search warrant may be issued. A court shall issue a criminal seizure warrant if it determines that the property to be seized would, in the event of a conviction, be subject to forfeiture, and that a restraining order would be inadequate to assure the availability of the property for forfeiture.

38. Neither a restraining order nor an injunction is sufficient to guarantee the availability of the **SUBJECT DOMAIN NAME** for forfeiture. By seizing the **SUBJECT DOMAIN NAME** and redirecting it to another website, the Government will prevent third

parties from acquiring the name and using it to commit additional crimes. Furthermore, seizure of the **SUBJECT DOMAIN NAME** will prevent third parties from continuing to access https://KingsmarkPharma.com/ in its present form.

39. Venue for civil forfeitures lies (1) in any district in which any of the acts or omissions giving rise to the forfeiture occurred pursuant to 28 U.S.C. Title 28, United States Code, Section 1355(b)(1)(A) (1); (2) in the district in which such property is found, pursuant to 28 U.S.C. § 1395(b); or (3) in any district where the defendant owning the property is located or in the judicial district where the criminal prosecution is brought pursuant to 18 U.S.C. § 981(h), as incorporated by 18 U.S.C. § 2323(a)(2).

40. As set forth above, there is probable cause to believe that the **SUBJECT DOMAIN NAME** is subject to civil and criminal forfeiture because it was used in the commission of trafficking in counterfeit goods or services, which were conducted in violation of 18 U.S.C. § 2320.

SEIZURE PROCEDURE

41. As detailed in ATTACHMENT A, upon execution of the seizure warrant, VeriSign Inc., the registry for the ".com" top-level domain (the **SUBJECT REGISTRY**), headquartered at 12061 Bluemont Way, Reston, VA 20190, shall be directed to restrain and lock the **SUBJECT DOMAIN NAME** pending transfer of all right, title, and interests in the **SUBJECT DOMAIN NAME** to the United States upon completion of forfeiture proceedings, to ensure that changes to the **SUBJECT DOMAIN NAME** cannot be made absent court order or, if forfeited to the United States, without prior consultation with HSI or DOJ.

42. In addition, upon seizure of the **SUBJECT DOMAIN NAME** by HSI, VeriSign

Inc., will be directed to associate the **SUBJECT DOMAIN NAME** to a new authoritative name server(s) to be designated by a law enforcement agent. The Government will display a notice on the website to which the **SUBJECT DOMAIN NAME** will resolve indicating that the site has been seized pursuant to a warrant issued by this court.

CONCLUSION

43. For the foregoing reasons, I submit that there is probable cause to believe that the **SUBJECT DOMAIN NAME** is used in and/or intended to be used in facilitating and/or committing the **SUBJECT OFFENSES**. Accordingly, the **SUBJECT DOMAIN NAME** is subject to forfeiture to the United States pursuant to 21 U.S.C. § 853, and 18 U.S.C. §§ 981(b), 2320, and 2323, and I respectfully request that the Court issue a seizure warrant for the **SUBJECT DOMAIN NAME**.

44. Because the warrant will be served on VeriSign Inc., which controls the **SUBJECT DOMAIN NAME**, thereafter, at a time convenient to it, will transfer control of the **SUBJECT DOMAIN NAME** to the Government, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

Digitally signed by RYAN M DIANDREA
Date: 2022.06.06 18:12:23 -04'00'

Special Agent Ryan DiAndrea
Homeland Security Investigations

Affidavit submitted by email and attested to me as true and accurate by telephone consistent with Fed. R. Crim. P. 4.1 and 41(d)(3) this 8th day of June, 2022.

A. David Copperthite

THE HONORABLE A. DAVID COPPERTHITE
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

With respect to "**KingsmarkPharma.com**" ("**SUBJECT DOMAIN NAME**"), VeriSign Inc., who is the domain registry for the **SUBJECT DOMAIN NAME**, shall take the following actions to effectuate the seizure of the **SUBJECT DOMAIN NAME**:

1) Take all reasonable measures to redirect the **SUBJECT DOMAIN NAME** to substitute servers at the direction of Department of Homeland Security - Homeland Security Investigations, by associating the **SUBJECT DOMAIN NAME** to the following authoritative name-server(s) or **by redirecting traffic to the SUBJECT DOMAIN NAME to the following IP addresses**:
    (a) Ns1.seizedservers.com (IP address 66.212.148.117);
    (b) Ns2. seizedservers.com (IP address 66.212.148.118); and/or
    (c) Any new authoritative name server or IP address to be designated by a law enforcement agent in writing, including e-mail, to the Subject Registrar.
2) Prevent any further modification to, or transfer of, the **SUBJECT DOMAIN NAME** pending transfer of all right, title, and interest in the **SUBJECT DOMAIN NAME** to the United States upon completion of forfeiture proceedings, to ensure that changes to the **SUBJECT DOMAIN NAME** cannot be made absent court order or, if forfeited to the United States, without prior consultation with the Department of Homeland Security.
3) Take all reasonable measures to propagate the necessary changes through the Domain Name System as quickly as practicable.
4) Provide reasonable assistance in implementing the Terms of this Order and take no unreasonable action to frustrate the implementation of this Order.

5) The Government will display a notice on the website to which the **SUBJECT DOMAIN NAME** will resolve. That notice will consist of law enforcement emblems and the following text (or substantially similar text):

> "This domain name has been seized in accordance with a seizure warrant issued by the United States Court for the District of Maryland after a Magistrate Judge found probable cause that the domain was forfeitable pursuant to 18 U.S.C. §§ 2320, 18 U.S.C. §§ 2323 and 18 U.S.C. §§ 981. Notice of forfeiture proceedings for this domain will be issued as set forth by law."

ATTACHMENT B

I. Seizure Procedure

A. The seizure warrant will be presented in person or transmitted via facsimile or email to personnel of the domain name registry listed in Section II ("Subject Registry") and the domain name registrars based in the United States listed in Section III ("Subject Registrars"). The Subject Registry will be directed, for the domain names listed in Section IV ("Subject Domain Names") for which it serves as the top-level domain registry, to make any changes necessary to restrain and lock the domain name pending transfer of all rights, title, and interest in the Subject Domain Name to the United States upon completion of forfeiture proceedings.

B. Upon seizure of the Subject Domain Names, the Subject Registry shall point the Subject Domain Names to the IPR Center's Domain Names ns1.seizedservers.com (IP address 66.212.148.117) and ns2.seizedservers.com (IP address 66.212.148.118) and at which the Government will display a web page with the following notice:

> *This domain name has been seized in accordance with a seizure warrant issued by the United States Court for the District of Maryland after a Magistrate Judge found probable cause that the domain was forfeitable pursuant to 18 U.S.C. §§ 2320, 18 U.S.C. §§ 2323 and 18 U.S.C. §§ 981. Notice of forfeiture proceedings for this domain will be issued as set forth by law.*

C. Upon seizure of the Subject Domain Names, the Subject Registry will take all steps necessary to restrain and lock the domain at the registry level to ensure that changes to the subject domain names cannot be made absent a court order or, if forfeited to the United States government, without prior consultation with United States Immigration and Customs Enforcement.

D. Upon seizure of the Subject Domain Names, the Subject Registrars based in the United States shall contact the registrant of the Subject Domain Name and provide them notice of the seizure along with the following contact information:

(a)	Name:	Homeland Security Investigations National Intellectual Property Rights Coordination Center
(b)	Address:	2451 Crystal Drive, Suite 200 Arlington, VA 20598-5105
	Country:	USA
(c)	Telephone:	1-866-IPR-2060 (477-2060)
(d)	Email:	IPRCenter@dhs.gov
(e)	Fax:	703-603-3872

II. Subject Registry

VeriSign, Inc.,
12061 Bluemont Way
Reston, VA 20190

III. Subject Registrars based in the U.S.

None

IV. Subject Domain Name(s):

KingsmarkPharma.com